PCT/JP2004/000677

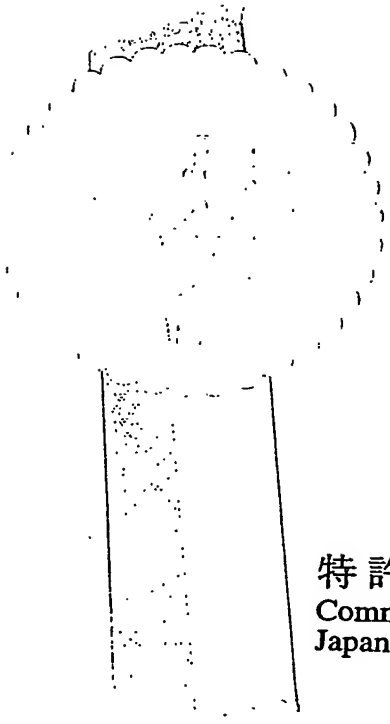
日本国特許庁 27.1.2004
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年 １月２７日

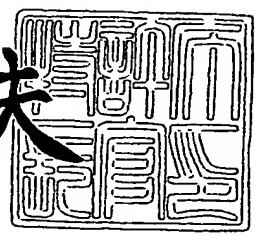
出願番号
Application Number: 特願２００３－０１７６３７
[ST. 10/C]: [ＪＰ２００３－０１７６３７]

出願人
Applicant(s): 松下電器産業株式会社



２００４年 ２月２６日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫



出証番号 出証特２００４－３０１３６０５

【書類名】　特許願
【整理番号】　2032750008
【あて先】　特許庁長官殿
【国際特許分類】　G06F　9/06
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　三浦　康史
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　徳田　克己
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デジタルコンテンツ配信システム

【特許請求の範囲】

【請求項１】　ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、

前記サーバ装置および前記端末装置間の通信に、少なくとも前記サーバ装置による前記端末装置の正当性の認証と通信暗号鍵の共有を行う認証フェーズを含み、

前記認証フェーズには、前記サーバ装置と前記端末装置間で通信されるトランザクションを識別する情報を交換するトランザクション識別情報交換フェーズと、前記トランザクションにおける前記端末装置からの先頭のコマンドを送信する先頭コマンド送信フェーズとを含むことにより、ユーザに対する応答時間を削減する

ことを特徴とするデジタルコンテンツ配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークを用いて、サーバ装置から映像、音楽などのデジタルコンテンツと、デジタルコンテンツの利用を許諾するライセンスを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、前記サーバ装置と前記端末装置間の通信において、不正にライセンスの複製や改ざんが行われることを防ぎつつ、通信切断発生時においてもライセンスの消失や二重配信をも防ぐシステムおよび装置に関する。

【０００２】

【従来の技術】

近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテンツと記述）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末

装置に配信し、端末装置においてコンテンツを利用することが可能な、コンテンツ配信システムと呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術等を用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。

【０００３】

例えば、特許文献１には、コンテンツ配信システムの一例として、暗号化されたコンテンツ、利用条件、および、コンテンツ復号鍵を端末装置が、サーバ装置より受信し、改ざん検出を行った後、利用条件の適合検証を行い、すべての検証を満足したときのみコンテンツの復号を行い出力するシステムが記載されている。

【０００４】

このように、従来のコンテンツ配信システムでは、サーバ装置からライセンス（利用条件とコンテンツ復号鍵の総称。利用権利とも呼ぶ）を端末装置に配信するが、その配信経路は一般的にインターネットなどの公衆回線を用いるため、ライセンスの盗聴および改ざんを防ぐ必要がある。つまり、利用条件の不正改ざんやコンテンツ鍵の流出を防止しなければならない。さらに、サーバ装置はライセンス配信先の認証も行う必要がある。つまり、サーバ装置が意図しない端末装置にライセンスを配信することも防止する必要がある。盗聴・改ざん防止と通信相手の認証を行うプロトコルはＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ）プロトコルと呼ばれ、例えば、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）がよく知られている（非特許文献１）。

【０００５】

また、通信装置・通信回線の故障や電源断などによる通信切断がライセンス配信中に発生した場合、そのライセンスが消失してしまう可能性がある。このような場合、購入したコンテンツを再生することができないといった不利益がユーザに発生する。例えば、特許文献２には、通信切断による通信データの消失を、デ

ータ再送によって回避するプロトコルが記載されている。

【０００６】

【特許文献１】

特開平７－１３１４５２号公報

【０００７】

【特許文献２】

特開２００２－２５１５２４号公報

【０００８】

【非特許文献１】

A.Frier, P.Karlton, and P.Kocher, “The SSL 3.0 Protocol”, [online], NetScape Communications Corp., Nov. 18, 1996, [平成15年１月１７日検索], インターネット＜URL: http://wp.netscape.com/eng/ssl3/draft302.txt＞

【０００９】

【発明が解決しようとする課題】

しかしながら、ＳＡＣプロトコルや通信切断対策プロトコルは、その適用範囲を広げるために汎用性を重視し、それぞれ独立に提案されている。これにより、双方のプロトコルを利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となるという課題があった。

【００１０】

より具体的には、ＳＡＣプロトコルは端末装置とサーバ装置との間で最少でも２往復の通信が必要であり、通信切断対策プロトコルは最少でも１往復の通信が必要である。つまり、ライセンス配信プロトコルを開始する前に、３回の通信往復回数が必要となる。それゆえ、端末装置がライセンスを取得するまでに通信往復４回分の通信遅延が発生し、ユーザがコンテンツ利用要求を出してから、コンテンツの利用開始までに待ち時間が発生するという課題があった。

【００１１】

本発明は、こうした従来の問題点を解決するものであり、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するととも

に、端末装置がライセンスを取得するまでの通信往復回数が２回であるプロトコルを実現するシステムおよび装置を提供することにより、ユーザがコンテンツの利用要求を出してから、コンテンツ利用開始までの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することを目的としている。

【００１２】

【課題を解決するための手段】

上記目的を達成するために、本発明に関わるコンテンツ配信システムは、ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、前記サーバ装置および前記端末装置間の通信に、少なくとも前記サーバ装置による前記端末装置の正当性の認証と通信暗号鍵の共有を行う認証フェーズを含み、前記認証フェーズには、前記サーバ装置と前記端末装置間で通信されるトランザクションを識別する情報を交換するトランザクション識別情報交換フェーズと、前記トランザクションにおける前記端末装置からの先頭のコマンドを送信する先頭コマンド送信フェーズとを含むことにより、ユーザに対する応答時間を削減することを特徴とする。

【００１３】

【発明の実施の形態】

（実施の形態１）

図１は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。図１において、本発明の一実施形態に係るコンテンツ配信システムは、サービス提供者側であるコンテンツ配信装置１と利用者側であるユーザ端末３とが、ネットワーク等の伝送路で接続される構成である。

【００１４】

コンテンツ配信装置１は、コンテンツ購入処理部１１と、ユーザ登録部１２と、ユーザ権利登録部１３と、ユーザ権利作成部１４と、コンテンツ暗号化部１５と、コンテンツ管理部１６と、セキュリティ管理／通信部１７と、ユーザデータベース１８と、コンテンツ権利データベース１９と、ユーザ所有権利データベー

ス２０と、コンテンツデータベース２１とを備えている。また、ユーザ端末３は、ユーザ指示処理部３１と、端末情報記憶部３２と、コンテンツ蓄積部３３と、利用権利管理部３４と、利用権利データベース３５と、セキュリティ管理／通信部３６と、出力部３７とを備えている。

【００１５】

まず、上記コンテンツ配信システムを構成するコンテンツ配信装置１およびユーザ端末３の概要を、以下に説明する。

コンテンツ配信装置１において、コンテンツ購入処理部１１は、コンテンツ購入処理実行時に、コンテンツ権利データベース１９に格納されている各コンテンツの内容、利用条件および料金等の情報を、ユーザ端末３へ送信してユーザに提示する。また、コンテンツ購入処理部１１は、ユーザによってコンテンツが購入された場合には、ユーザ端末３からユーザ情報（ユーザＩＤ、端末ＩＤ、ユーザ名、電話番号等）を取得すると共に、必要な課金処理を行う。コンテンツ権利データベース１９には、コンテンツ（映画やＴＶ放送等の動画、書籍や印刷物等の静止画、ラジオ放送や朗読等の音声および音楽、ゲーム等）毎に、コンテンツ利用に関する１つ又は複数の情報が格納されている。

【００１６】

ユーザ登録部１２は、コンテンツ購入処理部１１で取得されたユーザ情報を、ユーザデータベース１８に記憶して登録する。ユーザデータベース１８には、コンテンツ購入を行ったユーザの情報が、累積的に記憶されている。

【００１７】

ユーザ権利登録部１３は、ユーザ登録部１２を介してコンテンツ購入処理部１１から与えられる、ユーザが購入したコンテンツに関する情報を、ユーザが所有する権利としてユーザ所有権利データベース２０に記憶して登録する。ユーザ所有権利データベース２０には、ユーザが購入したコンテンツの利用権利が記憶されている。

【００１８】

ユーザ権利作成部１４は、ユーザ端末３から受けるコンテンツ利用要求に応じて、ユーザ端末３へ送信する利用権利（利用条件、コンテンツの復号鍵）を生成

する。

【００１９】

コンテンツ暗号化部１５は、ユーザ端末３へ送信するコンテンツの暗号化を行い、コンテンツデータベース２１へ暗号化コンテンツの登録を行う。

コンテンツ管理部１６は、ユーザ端末３へ送信する暗号化コンテンツをコンテンツデータベース２１から検索し、セキュリティ管理／通信部１７へ渡す。

【００２０】

セキュリティ管理／通信部１７は、ユーザ端末３の認証、コンテンツ配信装置１とユーザ端末３との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部１７の構成および通信プロトコルの詳細については後述する。

【００２１】

ユーザ端末３において、ユーザ指示処理部３１は、ユーザが入力する指示（コンテンツ購入要求やコンテンツ利用要求等の指示）を処理する。

端末情報記憶部３２には、上述したユーザ情報が記憶されている。

【００２２】

コンテンツ蓄積部３３には、購入によって取得された暗号化コンテンツが蓄積される。

利用権利管理部３４は、コンテンツ利用要求に応答してコンテンツ配信装置１から送信されてくる利用権利を受信し、その内容に従って、対応するコンテンツの処理（暗号解読や利用条件に基づく再生等）を実行する。この利用権利は、利用権利データベース３５に格納されて管理される。

【００２３】

出力部３７は、例えばディスプレイ等の表示装置であって、利用権利管理部３４が実行する処理に応じてコンテンツの出力を行う。

セキュリティ管理／通信部３６は、コンテンツ配信装置１の認証、コンテンツ配信装置１とユーザ端末３との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部３６の構成および通信プロトコルの詳細については後述する。

【００２４】

次に、コンテンツ配信装置１におけるセキュリティ管理／通信部１７の構成の詳細について図２を用いて説明する。固有鍵情報記憶部２０１は、公開鍵暗号方式におけるコンテンツ配信装置１固有の公開鍵ＫＤｓが含まれるサーバ公開鍵証明書と、コンテンツ配信装置１固有の秘密鍵ＫＥｓと、認証局公開鍵証明書とを記憶する。サーバ公開鍵証明書はコンテンツ配信装置１の公開鍵ＫＤｓに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、一般的なＸ．５０９証明書フォーマットを用いるものとする。公開鍵暗号方式およびＸ．５０９証明書フォーマットについては、カーライル・アダムズ他著、鈴木優一訳、「ＰＫＩ－公開鍵インフラストラクチャの概念、標準、展開」、ピアソンエデュケーション（２０００／７）が詳しい。

【００２５】

乱数発生部２０２は、乱数の生成を行う。生成された乱数は制御部２０４へ渡される。

暗号処理部２０３は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。データの暗号化および復号アルゴリズムにはＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を、署名生成および署名検証アルゴリズムにはＥＣ－ＤＳＡ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）を用いる。ＡＥＳについてはＮａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　Ｓｔａｎｄａｒｄ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｙ（ＮＩＳＴ）、ＦＩＰＳ　Ｐｕｂｌｉｃａｔｉｏｎ　１９７、ＥＣ－ＤＳＡについてはＩＥＥＥ　１３６３Ｓｔａｎｄａｒｄが詳しい。

【００２６】

暗号処理部２０３は、データの暗号化／復号を行う場合には、ＡＥＳ鍵と平文／暗号化データをそれぞれ入力とし、入力されたＡＥＳ鍵で暗号化／復号したデータをそれぞれ出力する。また、署名生成／検証を行う場合には、署名対象データ／署名検証データと公開鍵／秘密鍵をそれぞれ入力とし、署名データ／検証結果をそれぞれ出力する。さらに、セッション鍵生成用パラメータの生成を行う場

合には、乱数を入力とし、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータを出力する。また、セッション鍵の生成を行う場合、乱数とＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータを入力とし、セッション鍵を出力する。ここで、セッション鍵の生成にはＥＣ－ＤＨ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）を用いる。ＥＣ－ＤＨのアルゴリズムは、上記のＩＥＥＥ　１３６３　Ｓｔａｎｄａｒｄが詳しい。

【００２７】

制御部２０４は、ユーザ端末３の認証処理、ユーザ端末３と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部２０４は、トランザクション毎にトランザクション識別子を割り当て、そのトランザクション識別子を通信ログデータベース２０６に保存することにより、通信切断対策処理を行う。ここで、トランザクションとは、「利用権利の取得」や「利用権利の返却」などの処理単位を表す。

【００２８】

通信部２０５は、ユーザ端末３のセキュリティ管理／通信部３６と通信を行う。

次に、ユーザ端末３におけるセキュリティ管理／通信部３６の構成の詳細について図３を用いて説明する。固有鍵情報記憶部３０１は、公開鍵暗号方式におけるユーザ端末３固有の公開鍵ＫＤｃが含まれる端末公開鍵証明書と、ユーザ端末３固有の秘密鍵ＫＥｃと、認証局公開鍵証明書を記憶する。端末公開鍵証明書はユーザ端末３の公開鍵ＫＤｃに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、コンテンツ配信装置１と同様にＸ．５０９証明書フォーマットを用いる。

【００２９】

乱数発生部３０２は、乱数の生成を行う。生成された乱数は制御部３０４へ渡される。

暗号処理部３０３は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。暗号処理部３０３の入出力は、コンテンツ配信装置１の暗号処理部２０３と同じである。

【００３０】

制御部３０４は、コンテンツ配信装置１の認証処理、コンテンツ配信装置１と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部３０４は、コンテンツ配信装置１が生成したトランザクション識別子を通信ログデータベース３０６に蓄積することにより、通信切断対策処理を行う。

【００３１】

通信部３０５は、ユーザ端末３側のセキュリティ管理／通信部１７と通信を行う。

次に、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ配信方法を、図４～図１２を参照して具体的に説明する。

【００３２】

図４は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入に関する処理を説明するフローチャートである。図５は、コンテンツ権利データベース１９に格納されているコンテンツに関する情報の一例を概念的に示す図である。図６は、ユーザデータベース１８に格納されているユーザ情報の一例を概念的に示す図である。図７は、ユーザ所有権利データベース２０に格納されているユーザが所有する権利の情報の一例を概念的に示す図である。図８は、コンテンツデータベース２１に格納されているコンテンツ情報の一例を概念的に示す図である。図９は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。図１０～図１２は、本発明の一実施形態に係るコンテンツ配信システムで行われる秘匿通信と通信切断対策処理を説明するフローチャートである。

【００３３】

（１）コンテンツ購入処理

図４を参照して、コンテンツ配信装置１で提供されるコンテンツをユーザが購入する際に、コンテンツ配信システムで行われる処理を説明する。

【００３４】

ユーザ端末３では、ユーザが、コンテンツ購入に関する指示をユーザ指示処理部３１へ出力する。ユーザ指示処理部３１は、セキュリティ管理／通信部３６を

介して、指示に応じたコンテンツ購入要求をコンテンツ配信装置１へ発行する（ステップＳ４１）。

【００３５】

コンテンツ配信装置１では、ユーザ端末３から発行されたコンテンツ購入要求が、セキュリティ管理／通信部１７を介してコンテンツ購入処理部１１で受信される。コンテンツ購入処理部１１は、コンテンツ購入要求を受信すると、コンテンツ権利データベース１９から格納されているすべてのコンテンツに関する情報を取得し、セキュリティ管理／通信部１７を介してユーザ端末３へ送信する（ステップＳ４２）。

【００３６】

ここで、コンテンツ権利データベース１９には、例えば図５に示すような情報が格納されている。図５において、コンテンツ名は、コンテンツの名称であり、コンテンツＩＤは、コンテンツを識別するために付される固有の番号である。利用条件は、通常使用される予め定めたデータ形式によって、コンテンツを利用できる具体的な条件を示すものである。各コンテンツに設定される利用条件および金額は、１つであってもよいし、複数であってもよい。この例では、映画Ａというコンテンツには、再生回数による利用条件が設定されており、４００円を支払えば、映画Ａを２回観賞することができることを表している。

【００３７】

なお、利用条件には、上述した利用回数や利用時間以外にも、利用期間、記録媒体へのコピーや書面への印刷の可否等の様々な条件を使用することが可能である。

【００３８】

再び図４を参照して、ユーザ端末３において、コンテンツ購入処理部１１から送信されたコンテンツに関する情報（図５）が確認され、ユーザがいずれかのコンテンツの購入を決定した場合（ステップＳ４３，Ｙｅｓ）、ユーザ指示処理部３１は、コンテンツ購入決定通知（購入したコンテンツおよび選択した利用条件の情報を含む）と共に、端末情報記憶部３２に格納されているユーザ情報を、セキュリティ管理／通信部３６を介してコンテンツ配信装置１へ送信する（ステッ

プＳ４４）。

【００３９】

コンテンツ配信装置１では、ユーザ端末３から送信されるコンテンツ購入決定通知およびユーザ情報を、セキュリティ管理／通信部１７を介してコンテンツ購入処理部１１で受信する。そして、コンテンツ購入処理部１１は、必要な課金処理を実行すると共に、購入されたコンテンツの情報とユーザ情報とを、ユーザ登録部１２へ送出する（ステップＳ４５）。なお、課金処理は本発明の主眼ではないので、説明を省略する。

【００４０】

ユーザ登録部１２は、コンテンツ購入処理部１１から送出される購入されたコンテンツの情報およびユーザ情報を、ユーザ権利登録部１３へ転送すると共に、ユーザ情報をユーザデータベース１８に記憶して登録する（ステップＳ４７）。このとき、コンテンツ購入処理部１１から送出されるユーザ情報と同一の内容が、既にユーザデータベース１８に登録されている場合には、上述したユーザ登録は行われない（ステップＳ４６，Ｙｅｓ）。

【００４１】

ユーザデータベース１８には、例えば図６に示すような情報が格納される。図６において、ユーザＩＤは、ユーザを識別するために付される固有の番号である。ユーザ名は、ユーザの名前である。端末ＩＤは、端末を識別するために付される固有の番号であり、１人のユーザが複数の端末を所有している場合等に利用される。電話番号は、ユーザを特定するために利用される。図６の例では、“ＩＤ番号「０００１」である「一朗」というユーザが、ＩＤ番号「１２３４５６７」の端末を利用する”という内容が、ユーザ情報として登録されている。

【００４２】

ユーザ権利登録部１３は、購入によってユーザが所有することになるコンテンツ利用の権利を、ユーザ登録部１２から与えられる購入されたコンテンツの情報とユーザ情報とに基づいて、ユーザ所有権利データベース２０に記憶して登録する（ステップＳ４８）。

【００４３】

ユーザ所有権利データベース２０には、例えば図７に示すような情報が格納されている。図７において、ユーザＩＤは、ユーザデータベース１８に登録されている情報である。コンテンツＩＤおよび利用条件は、コンテンツ権利データベース１９に登録されている情報である。

【００４４】

上記処理によって、コンテンツの購入およびその購入に伴うユーザの所有権利の登録が完了する。

（２）コンテンツ利用処理

次に、図９を参照して、上述した処理によってユーザ所有権利データベース２０にユーザ所有権利が登録された後、ユーザが購入したコンテンツを利用する際にコンテンツ配信システムで行われる処理を説明する。

【００４５】

ユーザ端末３では、ユーザが、コンテンツ利用に関する指示をユーザ指示処理部３１へ出力する。このとき、ユーザは、コンテンツをどのように利用するのかの指示を与える。例えば、購入したコンテンツの利用条件が回数であれば何回利用したいのか、時間であれば何分利用したいのかという指示を与える。ユーザ指示処理部３１は、セキュリティ管理／通信部３６を介して、指示に応じたコンテンツ利用要求をコンテンツ配信装置１へ送信する（ステップＳ９１）。なお、コンテンツ利用要求は、必ずしもユーザ指示に従って作成されるものではなく、ユーザ端末３内で自動的に作成される場合もある。例えば、端末３がサポートするコンテンツの利用条件が固定されている場合、ユーザが指示を与えるまでもなく、コンテンツ利用要求をユーザ端末３内で作成することができる。具体的には、ユーザ端末３が、記憶容量の制限により毎回１回分の利用権利だけが取得・処理可能な端末の場合であり、この場合には端末に応じたコンテンツ利用要求をユーザ指示処理部３１で自動的に作成し、コンテンツ配信装置１へ発行する。このコンテンツ利用要求には、上記指示の内容、ユーザＩＤ、端末ＩＤおよびコンテンツＩＤが含まれる。

【００４６】

コンテンツ配信装置１では、ユーザ端末３から送信されたコンテンツ利用要求

を、セキュリティ管理／通信部１７を介してユーザ権利作成部１４で受信する。ユーザ権利作成部１４は、コンテンツ利用要求を受信すると、この要求に対応した内容が登録されているか否かを、ユーザデータベース１８およびユーザ所有権利データベース２０を参照して確認する（ステップＳ９２）。具体的には、ユーザ権利作成部１４は、コンテンツ利用要求に含まれるユーザＩＤおよび端末ＩＤが、ユーザデータベース１８に登録されているか否かをまず確認し、登録されていると判断すると、そのユーザＩＤにおいてコンテンツ利用要求に含まれるコンテンツＩＤおよび指示に応じた利用条件が、ユーザ所有権利データベース２０に登録されているか否かを確認する。

【００４７】

上記ステップＳ９２における確認の結果、コンテンツ利用要求に対応した内容が登録されていると判断した場合（ステップＳ９３，Ｙｅｓ）、ユーザ権利作成部１４は、コンテンツ利用要求に応じた利用権利を作成し、セキュリティ管理／通信部１７を介してユーザ端末３へ送信する（ステップＳ９４）。また、ユーザ権利作成部１４は、コンテンツ利用要求に含まれるコンテンツＩＤをコンテンツ管理部１６へ通知する。コンテンツ管理部１６は、コンテンツＩＤに対応するコンテンツをコンテンツデータベース２１から取り出し、セキュリティ管理／通信部１７を介してユーザ端末３へ送信する（ステップＳ９５）。

【００４８】

一方、上記ステップＳ９２における確認の結果、コンテンツ利用要求に対応した内容が登録されていないと判断した場合（ステップＳ９３，Ｎｏ）、ユーザ権利作成部１４は、コンテンツ利用要求を拒絶する旨を、セキュリティ管理／通信部１７を介してユーザ端末３へ通知する（ステップＳ９７）。

【００４９】

ここで、上記ステップＳ９４で行われる利用権利の生成は、次のようにして行われる。前提として、ユーザＩＤ「０００１」のユーザが、図７のユーザ所有権利データベース２０に示される登録内容で、事前にコンテンツの購入を行っていたと仮定する。

【００５０】

さらに、そのユーザが、コンテンツＩＤ「１１２２３３」のコンテンツを１回利用したいというコンテンツ利用要求を送信してきた場合を考える。この場合、ユーザ所有権利データベース２０に登録されている利用条件が２回であるので、ユーザ権利作成部１４は、要求通り再生回数＝１を与える情報および該当コンテンツの復号鍵を含む利用権利を作成する。また、ユーザ権利作成部１４は、この利用権利の作成と同時に、ユーザ所有権利データベース２０に登録されている利用条件の回数を１つ減少させて、登録内容を更新する（図７の例では、２→１）。ただし、通信切断対策処理において、セキュリティ管理／通信部１７から再開トランザクションとして指示された場合には、登録内容の更新を行わない。なお、通信切断対策処理については後述する。

【００５１】

なお、ユーザ権利作成部１４は、通信切断対策処理により再開トランザクションが発行されることを想定して、作成したユーザ権利を保存しておいてもよい。これにより、再開トランザクション発行時にユーザ権利を再度作成する手間を省くことができる。

【００５２】

なお、ユーザ端末３へ利用権利を発行する毎に、ユーザ所有権利データベース２０に登録されている内容を更新した結果、コンテンツの購入によって与えられた利用条件がなくなった場合には、ユーザ所有権利データベース２０に登録されている該当ユーザ所有権利を削除してもよいし、そのまま残しておいてもよい。残しておく場合には、同一のユーザが再度同じコンテンツの購入を行ったときや、ユーザが取得した利用権利を行使せずに返却するとき等に、処理対応がしやすくなる。

【００５３】

再び図９を参照して、ユーザ端末３において、コンテンツ配信装置１から送信される暗号化コンテンツは、コンテンツ蓄積部３３に蓄積され、利用権利は、利用権利管理部３４に入力される。利用権利管理部３４は、取得した利用権利に含まれる復号鍵を用いて該当コンテンツに施された暗号を解読し、利用条件に従って暗号解読したコンテンツの再生処理等を、出力部３７を通して実行する（ステ

ップＳ９６）。なお、取得された利用権利は、利用権利データベース３５に格納され、コンテンツの再生回数や累積時間等の管理に利用される。

【００５４】

上記処理によって、要求される利用条件に応じたコンテンツを配信することができる。

（３）秘匿通信・通信切断処理

次に、図１０～図１２を参照して、上述したコンテンツ利用処理において、利用権利の要求（図９のステップＳ９１）、および、利用権利の配信（図９のステップＳ９５）の際に、セキュリティ管理／通信部１７、３６で行われる、ユーザ端末３の認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理を説明する。

【００５５】

図１０は、コンテンツ利用処理におけるユーザ端末３とコンテンツ配信装置１との１回目の通信往復で行われる処理について記述している。また、図１１は、前記１回目の通信往復後、２回目の通信往復を開始する前にユーザ端末３において行われる処理について記述している。さらに、図１２はコンテンツ利用処理におけるユーザ端末３とコンテンツ配信装置１との２回目の通信往復で行われる処理について記述している。

【００５６】

ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、ユーザ指示処理部３１からコンテンツ利用要求の送信を指示された場合、乱数発生部３０２で生成した乱数Ｒｃと、固有情報記憶部３０１に記憶している端末公開鍵証明書と、コンテンツ利用要求とを、通信部３０５を介して、コンテンツ配信装置１へ送信する（ステップＳ１００１）。

【００５７】

コンテンツ配信装置１のセキュリティ管理／通信部１７に含まれる制御部２０４は、通信部２０５を介してユーザ端末３から、乱数Ｒｃ、端末公開鍵証明書、コンテンツ利用要求を受信すると、まず、固有情報記憶部２０１に記憶している認証局公開鍵証明書と、前記端末公開鍵証明書とを、暗号処理部２０３に与える

ことにより、前記端末公開鍵証明書の署名検証を行う（ステップＳ１００２）。

【００５８】

上記ステップＳ１００２における署名検証の結果、検証失敗となった場合（ステップＳ１００３，Ｎｏ）、制御部２０４は、コンテンツ利用要求を拒絶する旨を、通信部２０５を介してユーザ端末３へ通知する（ステップＳ１００４）。

【００５９】

一方、上記ステップＳ１００２における署名検証の結果、検証が成功した場合（ステップＳ１００３，Ｙｅｓ）、制御部２０４は、乱数生成部２０２で乱数Ｒｓ、ＴＩＤ、およびＲｓ２を生成し、暗号処理部２０３で、乱数Ｒｓ２を入力としてＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｓの生成を行う（ステップＳ１００５）。ここでＴＩＤは、このコンテンツ要求トランザクションに対応付けられた識別子であり、今後、通信切断が発生した場合には、このトランザクション識別子ＴＩＤを用いて、中断されたトランザクションの再開が行われる。

【００６０】

さらに、制御部２０４は、ユーザ端末３から受信した乱数Ｒｃ、ステップＳ１００５で生成したＴＩＤ、ステップＳ１００５で生成したＤＨｓを連結したデータ（式１）の署名（式２）を暗号処理部２０３で生成する（ステップＳ１００６）。

Ｒｃ||ＴＩＤ||ＤＨｓ　　（式１）

Ｓ（ｓ，Ｒｃ||ＴＩＤ||ＤＨｓ）　　（式２）

【００６１】

制御部２０４は、ステップＳ１００５で生成した乱数Ｒｓ、トランザクション識別子ＴＩＤ、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｓと、固有鍵情報記憶部２０１に記憶しているサーバ公開鍵証明書と、ステップＳ１００６で生成した署名（式２）をユーザ端末３に通信部２０５を介して送信する（ステップＳ１００７）。

【００６２】

ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、通信部３０５を介してコンテンツ配信装置１から、乱数Ｒｓ、トランザクション識

別子ＴＩＤ、Ｄｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｓ、サーバ公開鍵証明書、および署名データを受信すると、まず、固有情報記憶部３０１に記憶している認証局公開鍵証明書と、前記サーバ公開鍵証明書とを、暗号処理部３０３に与えることにより、前記サーバ公開鍵証明書の署名検証を行う（ステップＳ１１０１）。

【００６３】

上記ステップＳ１１０１における署名検証の結果、検証失敗となった場合（ステップＳ１１０２，Ｎｏ）、制御部３０４は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部３１へ通知する（ステップＳ１１０３）。

【００６４】

一方、上記ステップＳ１１０１における署名検証の結果、検証が成功した場合（ステップＳ１１０２，Ｙｅｓ）、制御部３０４は、ステップＳ１００１で作成した乱数ＲｃとステップＳ１００７でコンテンツ配信装置１から受信したＴＩＤ、およびＤＨｓを結合したデータ（式３）を生成し、そのデータ（式３）、ステップＳ１００７でコンテンツ配信装置１から受信した署名データ（式２）、およびサーバ公開鍵証明書を暗号処理部３０３に入力し、署名データ（式２）の検証を行う（ステップＳ１１０４）。

Ｒｃ||ＴＩＤ||ＤＨｓ　　（式３）

【００６５】

上記ステップＳ１１０４における署名検証の結果、検証失敗となった場合（ステップＳ１１０５，Ｎｏ）、制御部３０４は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部３１へ通知する（ステップＳ１１０３）。

【００６６】

一方、上記ステップＳ１１０４における署名検証の結果、検証が成功した場合（ステップＳ１１０５，Ｙｅｓ）、ユーザ端末３は通信相手が確かにコンテンツ配信装置１であることがわかる（通信相手の認証）。制御部３０４は、乱数発生部３０２で生成した乱数Ｒｃ２を暗号処理部３０３の入力としてＤｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｃを生成する（ステップＳ１１０６）。

【００６７】

さらに、制御部３０４は、ステップＳ１００７でコンテンツ配信装置１から受信したＤＨｓと、ステップＳ１１０６で生成したＲｃ２とから、暗号処理部３０３でセッション鍵ＫＳを生成する（ステップＳ１１０７）。

【００６８】

その後、制御部３０４は、ステップＳ１００７でコンテンツ配信装置１から受信したＴＩＤとＲｓ、ステップＳ１１０６で生成したＤＨｃとＫＳを通信ログデータベース３０６に記憶する（ステップＳ１１０８）。これにより、ＴＩＤに対応するコンテンツ利用権利要求トランザクションが、このステップまで完了したことがデータベースに保存される。よって、これ以降、通信切断などによりトランザクションが中断された場合には、この次のステップから処理を再開すればよいこととなる。

【００６９】

制御部３０４は、コンテンツ配信端末１から受信した乱数ＲｓとＴＩＤ、ステップＳ１１０６で生成したＤＨｃを連結したデータ（式４）の署名（式５）を暗号処理部３０３で生成する（ステップＳ１１０９）。

Ｒｓ||ＴＩＤ||ＤＨｃ　　（式４）

Ｓ（ｃ，Ｒｓ||ＴＩＤ||ＤＨｃ）　　（式５）

【００７０】

制御部３０４は、ＴＩＤと、ステップＳ１１０６で生成したＤＨｃと、ステップＳ１１０９で生成した署名（式５）をコンテンツ配信装置１に通信部３０５を介して送信する（ステップＳ１１１０）。

【００７１】

コンテンツ配信装置１のセキュリティ管理／通信部１７に含まれる制御部２０４は、通信部２０５を介してユーザ端末３から、トランザクション識別子ＴＩＤ、Ｄｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｃ、および署名データを受信すると、ステップＳ１００５で作成した乱数ＲｓとステップＳ１１１０でユーザ端末３から受信したＴＩＤ、およびＤＨｃを結合したデータ（式６）を生成し、そのデータ（式６）、ステップＳ１１１０でユーザ端末３から受信した署名データ、および端末公開鍵証明書を暗号処理部２０３に入力し、署名データの検証を行

う（ステップＳ１２０１）。

Ｒｓ｜｜ＴＩＤ｜｜ＤＨｃ　　（式６）

【００７２】

上記ステップＳ１２０１における署名検証の結果、検証失敗となった場合（ステップＳ１２０２，Ｎｏ）、制御部２０４は、コンテンツ利用要求を拒絶する旨を、通信部２０５を介してユーザ端末３へ通知する（ステップＳ１２０３）。

【００７３】

一方、上記ステップＳ１２０１における署名検証の結果、検証が成功した場合（ステップＳ１２０２，Ｙｅｓ）、コンテンツ配信装置１は通信相手が確かにユーザ端末３であることがわかる（通信相手の認証）。制御部２０４は、ステップＳ１２０１でユーザ端末３から受信したＤＨｃと、ステップＳ１００５で生成したＲｓ２とから、暗号処理部２０３でセッション鍵ＫＳを生成する（ステップＳ１２０４）。

【００７４】

さらに、制御部２０４は、通信ログデータベースを検索し、ステップＳ１２０１でユーザ端末３から受信したＴＩＤが存在するかを調べる。その結果、ＴＩＤが既に存在しない場合（ステップＳ１２０５，Ｎｏ）、制御部２０４は、ステップＳ１２０１でユーザ端末３から受信したＴＩＤと、ステップＳ１２０４で生成したＫＳを通信ログデータベース２０６に記憶する（ステップＳ１２０６）。これにより、ＴＩＤに対応するコンテンツ利用権利要求トランザクションが、このステップまで完了したことがデータベースに保存される。よって、これ以降、通信切断などによりトランザクションが中断された場合には、この次のステップから処理を再開すればよいこととなる。

【００７５】

その後、制御部２０４はユーザ権利生成部１４に新規トランザクションとして、ステップＳ１００１でユーザ端末３から受信したコンテンツ利用要求を通知する（ステップＳ１２０７）。

【００７６】

一方、ＴＩＤが既に存在する場合（ステップＳ１２０５，Ｙｅｓ）、制御部２

０４は、ユーザ権利生成部１４に再開トランザクションとして、ステップＳ１００１でユーザ端末３から受信したコンテンツ利用要求を通知する（ステップＳ１２０８）。

【００７７】

制御部２０４は、ＴＩＤとユーザ権利作成部１４で作成された利用権利を結合し、さらに、ステップＳ１２０４で生成したセッション鍵ＫＳを用いて暗号処理部２０３で暗号化して、通信部２０５を介してユーザ端末３に送信する(ステップＳ１２０９)。ここで、送信される利用権利は、コンテンツ配信端末１とユーザ端末３のみで生成可能なセッション鍵ＫＳで暗号化されているため、第三者が盗聴することはできない。

【００７８】

最後に、ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、通信部３０５を介してコンテンツ配信装置１から、暗号化データを受信すると、まず、暗号処理部３０３でセッション鍵ＫＳを用いて暗号化データの復号を行い、ＴＩＤと利用権利を復元する。さらに、通信ログデータベース３０６から、暗号化データに含まれるＴＩＤに対応するデータを削除する。（ステップＳ１２１０）。

【００７９】

上記処理により、ユーザ端末の認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理を行うことが可能となる。

なお、上記処理の完了後、ユーザ端末３は、コンテンツ配信装置１の通信ログデータベース２０６に保存されている不要な情報を削除するため、トランザクション完了通知をコンテンツ配信装置１に送信してもよい。トランザクション完了通知は完了したトランザクションのＴＩＤをセッション鍵ＫＳで暗号化したものである。トランザクション完了通知を受信したコンテンツ配信装置１は、ＴＩＤに対応するデータを通信ログデータベース２０６から削除する。

【００８０】

なお、本実施の形態で用いた暗号アルゴリズム、セッション鍵共有アルゴリズム、証明書フォーマットなどは、同等の機能を持つものであれば、必ずしも記載

したものを用いる必要はない。例えば、データの暗号アルゴリズムにはＴｒｉｐｌｅＤＥＳを用いてもよい。また、公開鍵暗号方式の代わりに共通鍵暗号方式を用いてもよい。

【００８１】

なお、本実施の形態では、ユーザ端末３からのコンテンツ利用要求と端末公開鍵証明書は、１往復目の通信（図１０のステップＳ１００１）において送信したが、２往復目の通信（図１１のステップＳ１１１０）において送信してもよい。これにより、コンテンツ配信装置１は、装置内に上記データを保持しておく必要がなくなる。この場合、コンテンツ配信装置１での端末公開鍵証明書の署名検証処理（図１０のステップＳ１１０２）は、２往復目の最初（図１２のステップＳ１２０１の直前）で行うこととなる。

【００８２】

なお、ステップＳ１００７において、コンテンツ配信装置１からユーザ端末３へ送信されるデータに、ユーザ端末３から受信した乱数Ｒｃを含めてもよい。つまり、コンテンツ配信装置１から送信されるデータは、乱数Ｒｃ、乱数Ｒｓ、ＴＩＤ、パラメータＤＨｓ、署名データとなる。これにより、ユーザ端末３は、乱数Ｒｃを端末内に保持しておく必要がなくなる。同様に、ステップＳ１１１０において、ユーザ端末３からコンテンツ配信端末１へ送信されるデータに、コンテンツ配信装置１から受信した乱数Ｒｓを含めてもよい。つまり、コンテンツ配信装置１から送信されるデータは、乱数Ｒｓ、ＴＩＤ、パラメータＤＨｃ、署名データとなる。

【００８３】

なお、本実施の形態において、ＴＩＤはコンテンツ配信装置１が生成したが、ユーザ端末３で生成してもよい。この場合、ステップＳ１００１において、ユーザ端末３はコンテンツ配信装置１に対して、生成したＴＩＤを送信する。

【００８４】

なお、本実施の形態においては、ユーザ端末３がコンテンツ配信装置１を認証する処理も含まれているが、特に必要がない場合には、認証処理を除いてもよい。

【００８５】

なお、本実施の形態においては、ステップＳ９４においてユーザ権利の作成を行う際に、セキュリティ管理／通信部１７から再開トランザクションとして指示された場合には、登録内容の更新を行わないとしたが、再度、コンテンツ利用要求を評価し、ユーザ権利の作成をやり直してもよい。これにより、新規トランザクションの発行と再開トランザクションの発行の間に起こった状況変化に対応することが可能となる。例を挙げれば、新規トランザクション発行時には、コンテンツの利用有効期限内であったので利用権利の作成・送信を行なったが、再開トランザクションとして再度要求が行われたときには、コンテンツの利用有効期限を越えたいた場合が考えられる。この場合には、再開トランザクションに対しては利用権利の作成・発行は行わない。

【００８６】

なお、本実施の形態では、１つのトランザクション処理についての例を示したが、複数のトランザクション処理を行う場合には、例示した処理を複数回行えばよい。複数トランザクション処理において、さらに、応答時間を削減したい場合には、２回目以降の認証処理を除いてもよい。つまり、認証処理は最初の１度だけ行い、同じセッション鍵ＫＳを再利用する。さらに、複数のトランザクションを逐次的に実行するのではなく、並列的に実行してもよい。これにより、１トランザクションあたりの応答時間が削減される。

【００８７】

また、コンテンツ配信装置１とユーザ端末３との間の２つのコンテンツ利用要求処理を処理Ａおよび処理Ｂとするとき、処理Ａの終了後に、一旦、通信切断を行わなければいけない場合、通常は、処理Ｂの開始時には再度認証処理を行い、新たなセッション鍵を作成しなおすが、処理Ｂの応答時間を削減したい場合には、処理Ｂでの認証処理を除くために、処理Ａでのセッション鍵をコンテンツ配信装置１とユーザ端末３の双方で記憶しておき、再利用してもよい。

【００８８】

なお、上記のように、セッション鍵の再利用を行う際、コンテンツ配信装置１はセッション鍵の利用制限を設けてもよい。例えば、セッション鍵の再利用回数

が規定の上限を超えた場合、セッション鍵が最初に作成されたから規定の時間が経過した場合、セッション鍵が最初に作成されてから規定の通信データ量を超えた場合、予め決められたコンテンツあるいは利用権利を配信する場合、あるいは、予め決められたユーザ端末３に配信する場合などに、コンテンツ配信装置１はユーザ端末３にセッション鍵再利用不可通知を行う。セッション鍵再利用不可通知を受信したユーザ端末３は、セッション鍵を生成しなおす。つまり、ステップ１００１から通信をやり直す。

【００８９】

なお、本実施の形態で示したコンテンツ配信システムの各構成要素は、ハードウェアで実現しても、ソフトウェアで実現してもよい。

【００９０】

【発明の効果】

以上のように本発明によれば、ライセンスの盗聴･改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、端末装置がライセンスを取得するまでの通信往復回数が２回であるプロトコルを実現するシステムおよび装置を提供することにより、ユーザがコンテンツの利用要求を出してから、コンテンツ利用開始までの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図

【図２】

本発明の一実施形態に係るコンテンツ配信システムの構成のコンテンツ配信装置のセキュリティ管理／通信部を示すブロック図

【図３】

本発明の一実施形態に係るコンテンツ配信システムの構成のユーザ端末のセキュリティ管理／通信部を示すブロック図

【図４】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入

に関する処理を説明するフローチャート

【図５】

コンテンツ権利データベース１９に格納されているコンテンツに関する情報の一例を概念的に示す図

【図６】

ユーザデータベース１８に格納されているユーザ情報の一例を概念的に示す図

【図７】

ユーザ所有権利データベース２０に格納されているユーザが所有する権利の情報の一例を概念的に示す図

【図８】

コンテンツデータベース２１に格納されているコンテンツ情報の一例を概念的に示す図

【図９】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャート

【図１０】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１との１回目の通信往復で行われる処理を説明するフローチャート

【図１１】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１との１回目の通信往復後、２回目の通信往復を開始する前にユーザ端末３において行われる処理を説明するフローチャート

【図１２】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１との２回目の通信往復で行われる処理を説明するフローチャート

【符号の説明】

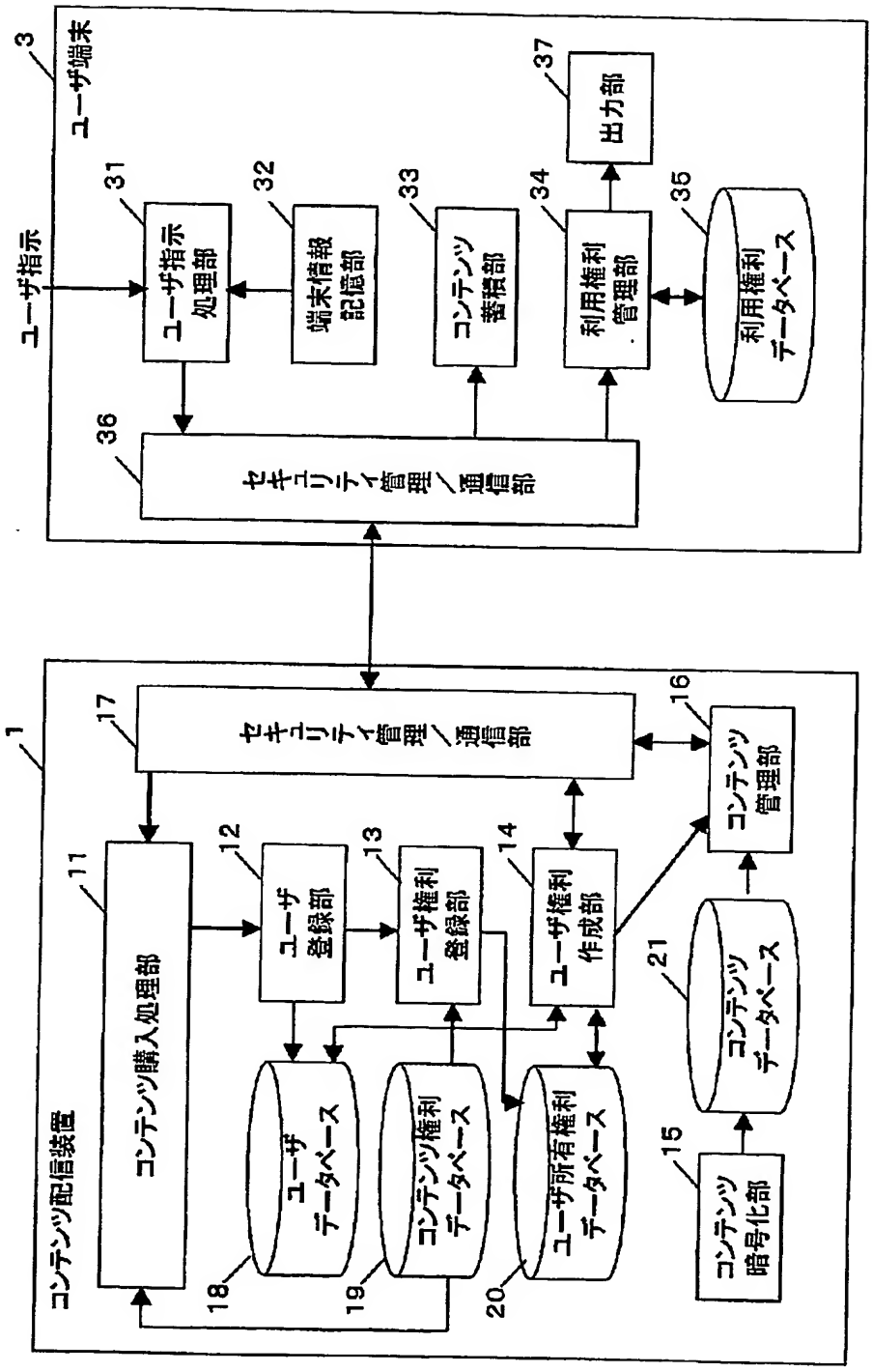
１	コンテンツ配信装置
３	ユーザ端末
１１	コンテンツ購入処理部
１２	ユーザ登録部
１３	ユーザ権利登録部
１４	ユーザ権利作成部
１５	コンテンツ暗号化部
１６	コンテンツ管理部
１７，３６	セキュリティ管理／通信部
１８	ユーザデータベース
１９	コンテンツ権利データベース
２０	ユーザ所有権利データベース
２１	コンテンツデータベース
３１	ユーザ指示処理部
３２	端末情報記憶部
３３	コンテンツ蓄積部
３４	利用権利管理部
３５	利用権利データベース
３７	出力部
２０１	固有鍵情報記憶部
２０２	乱数発生部
２０３	暗号処理部
２０４	制御部
２０５	通信部
２０６	通信ログデータベース
３０１	固有鍵情報記憶部
３０２	乱数発生部
３０３	暗号処理部
３０４	制御部

３０５　　通信部

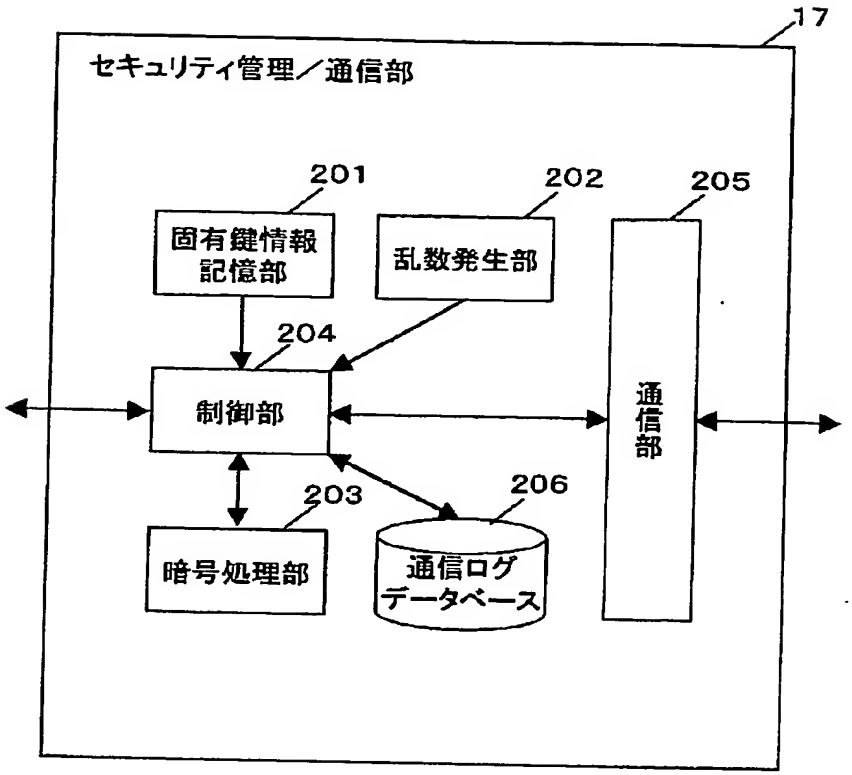
３０６　　通信ログデータベース

【書類名】　図面

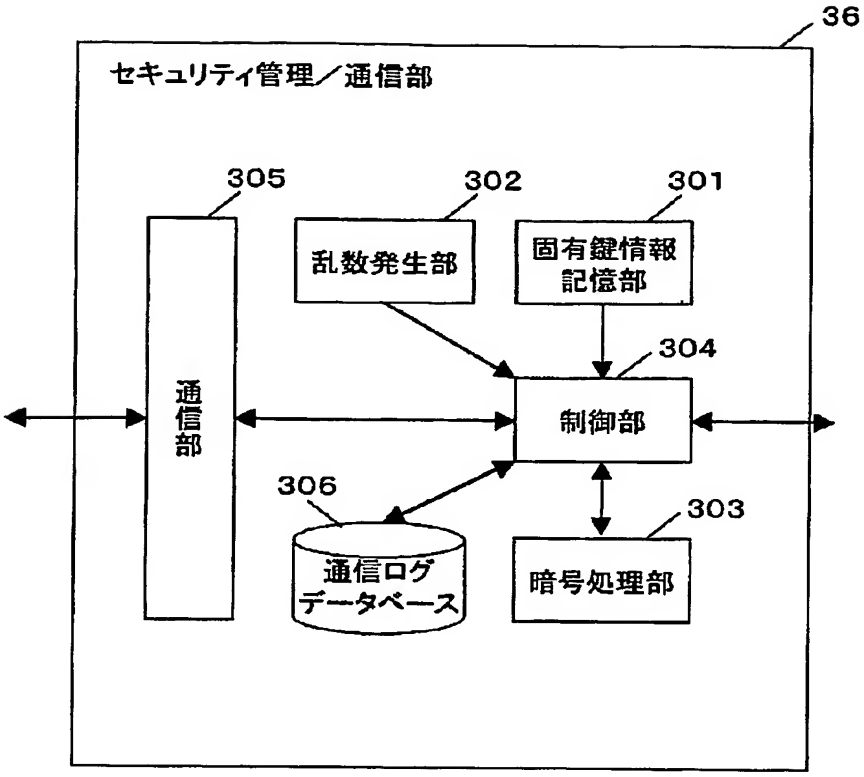
【図１】


3
ユーザ端末
ユーザ指示
31
ユーザ指示処理部
32
端末情報記憶部
33
コンテンツ蓄積部
34
利用権利管理部
35
利用権利データベース
37
出力部
36
セキュリティ管理／通信部
1
コンテンツ配信装置
17
セキュリティ管理／通信部
16
コンテンツ管理部
11
コンテンツ購入処理部
12
ユーザ登録部
13
ユーザ権利登録部
14
ユーザ権利作成部
21
コンテンツデータベース
15
コンテンツ暗号化部
18
ユーザデータベース
19
コンテンツ権利データベース
20
ユーザ所有権利データベース

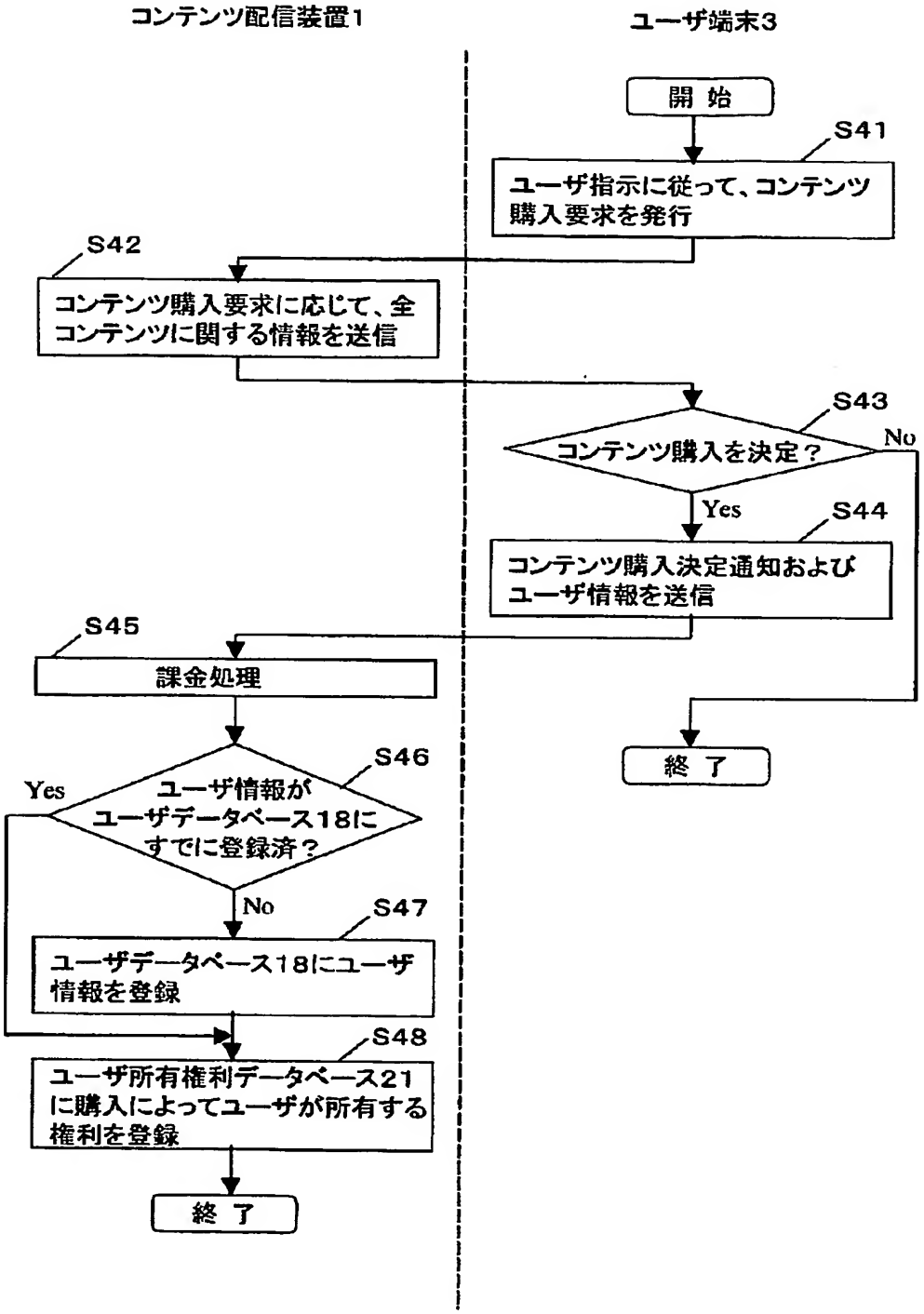
【図２】


17
セキュリティ管理／通信部
201
固有鍵情報記憶部
202
乱数発生部
205
204
制御部
通信部
203
206
暗号処理部
通信ログデータベース

【図３】


36
セキュリティ管理／通信部
305
302
301
乱数発生部
固有鍵情報記憶部
304
通信部
制御部
306
303
通信ログデータベース
暗号処理部

【図４】


コンテンツ配信装置1
ユーザ端末3
開 始
S41
ユーザ指示に従って、コンテンツ購入要求を発行
S42
コンテンツ購入要求に応じて、全コンテンツに関する情報を送信
S43
コンテンツ購入を決定？
No
Yes
S44
コンテンツ購入決定通知およびユーザ情報を送信
S45
課金処理
S46
Yes
ユーザ情報がユーザデータベース18にすでに登録済？
No
S47
ユーザデータベース18にユーザ情報を登録
S48
ユーザ所有権利データベース21に購入によってユーザが所有する権利を登録
終 了
終 了

【図５】

コンテンツ名	コンテンツID	利用条件	料金
映画A	112233	再生回数＝2	400円
音楽B	334567	再生回数＝5 累積再生時間＝1H	500円 1000円
ゲームC	321098	累積再生時間＝2H 無制限	700円 2000円

【図６】

ユーザID	ユーザ名	端末ID	電話番号
0001	一朗	1234567	06-XXXX-XXXX
0002	太郎	1170930	03-YYYY-YYYY

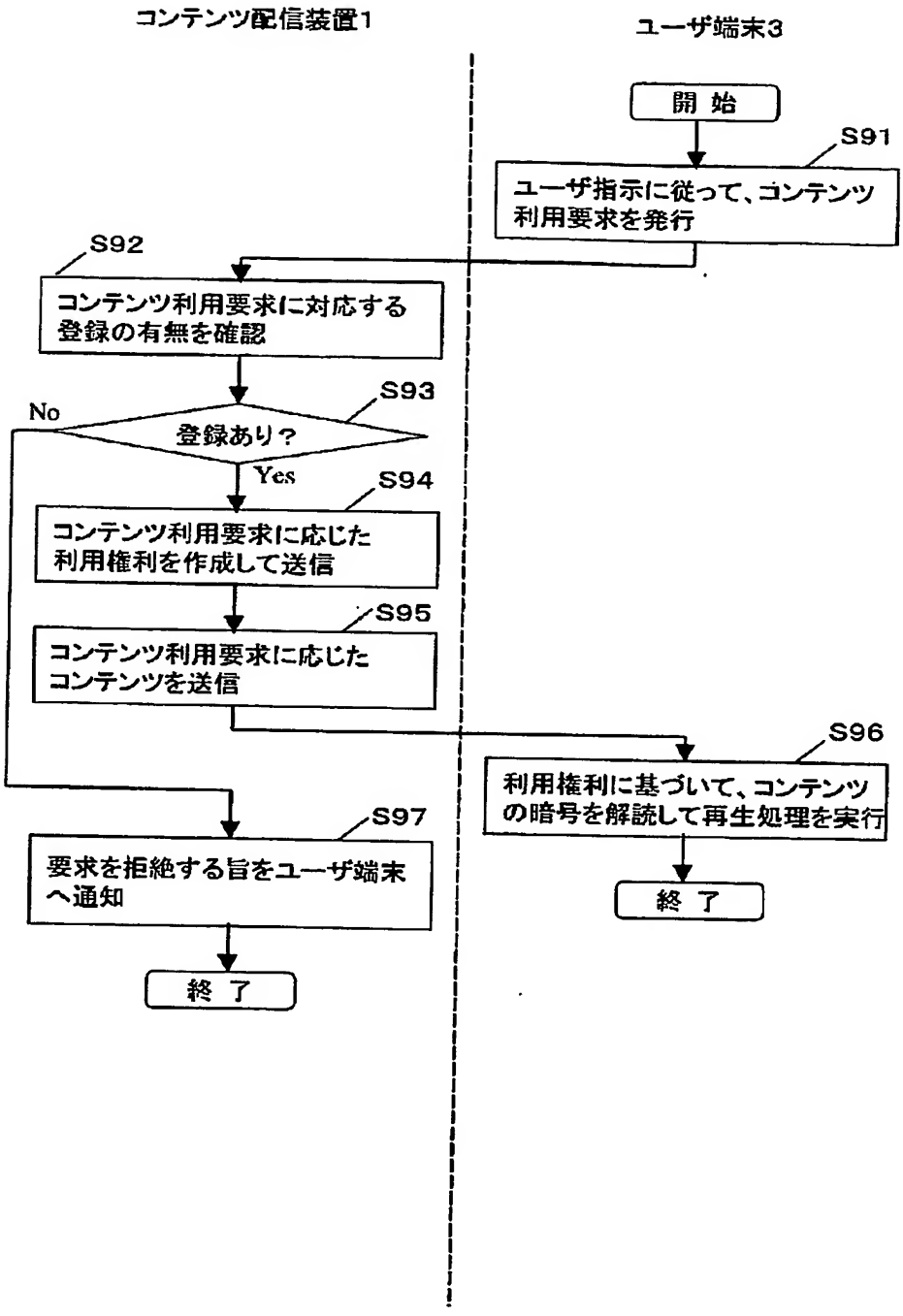
【図７】

ユーザID	コンテンツID	利用条件
0001	112233	再生回数＝2
0002	321098	累積再生時間＝2H

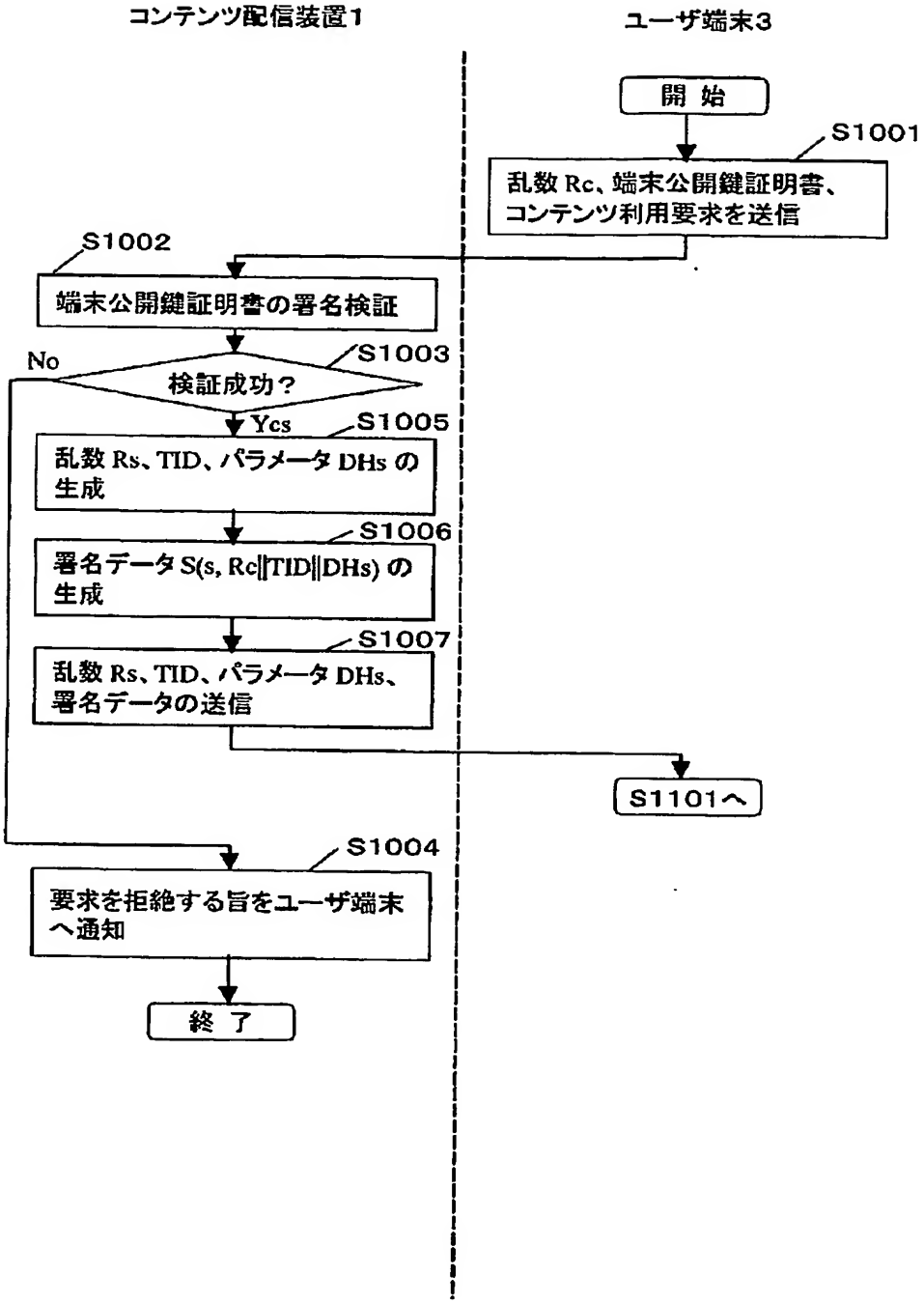
【図８】

コンテンツID	コンテンツ名	コンテンツ暗号鍵	ファイル名
112233	映画A	0123456789..	movieA.mpg
234567	音楽B	7361278168..	musicB.wav

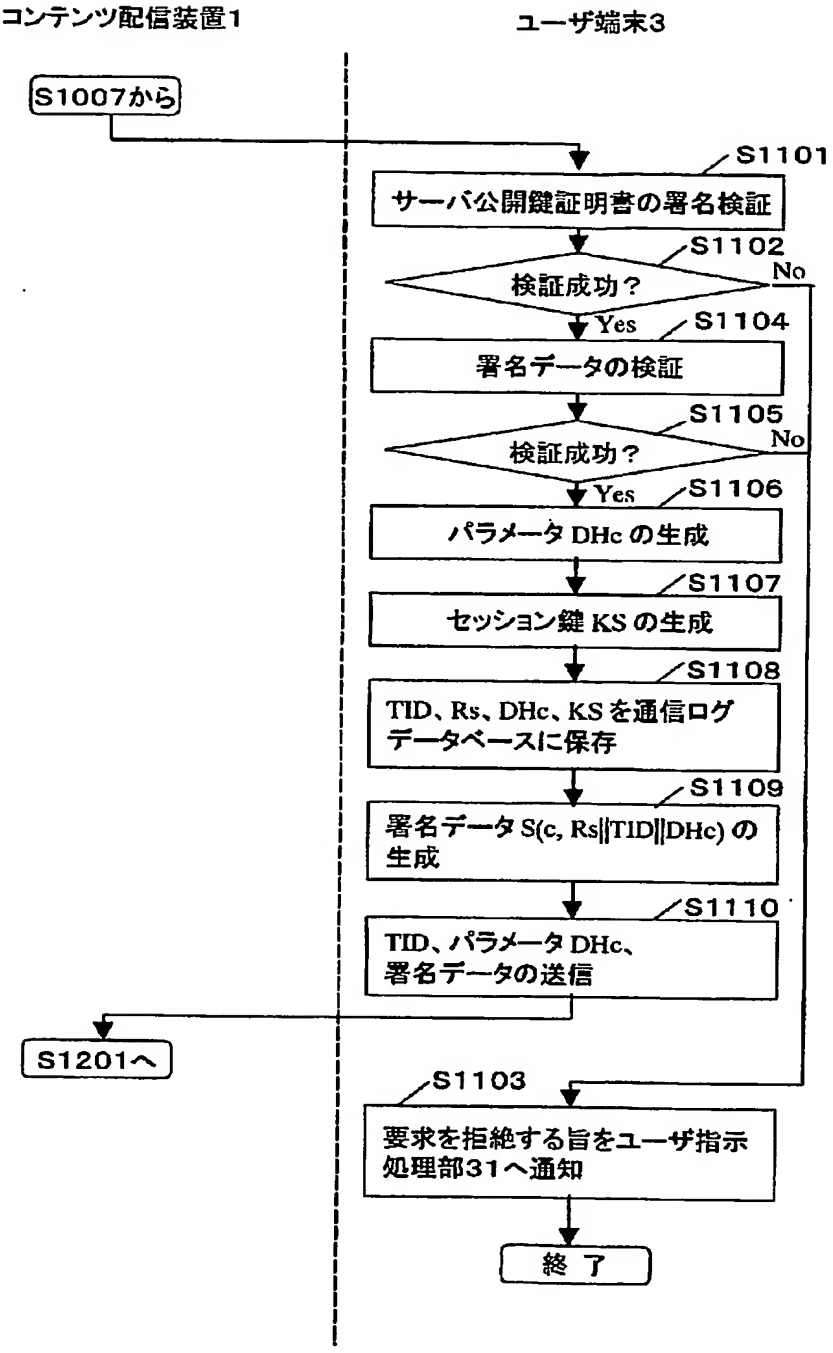
【図９】


コンテンツ配信装置1
ユーザ端末3
開 始
S91
ユーザ指示に従って、コンテンツ利用要求を発行
S92
コンテンツ利用要求に対応する登録の有無を確認
S93
No
登録あり？
Yes
S94
コンテンツ利用要求に応じた利用権利を作成して送信
S95
コンテンツ利用要求に応じたコンテンツを送信
S96
利用権利に基づいて、コンテンツの暗号を解読して再生処理を実行
終 了
S97
要求を拒絶する旨をユーザ端末へ通知
終 了

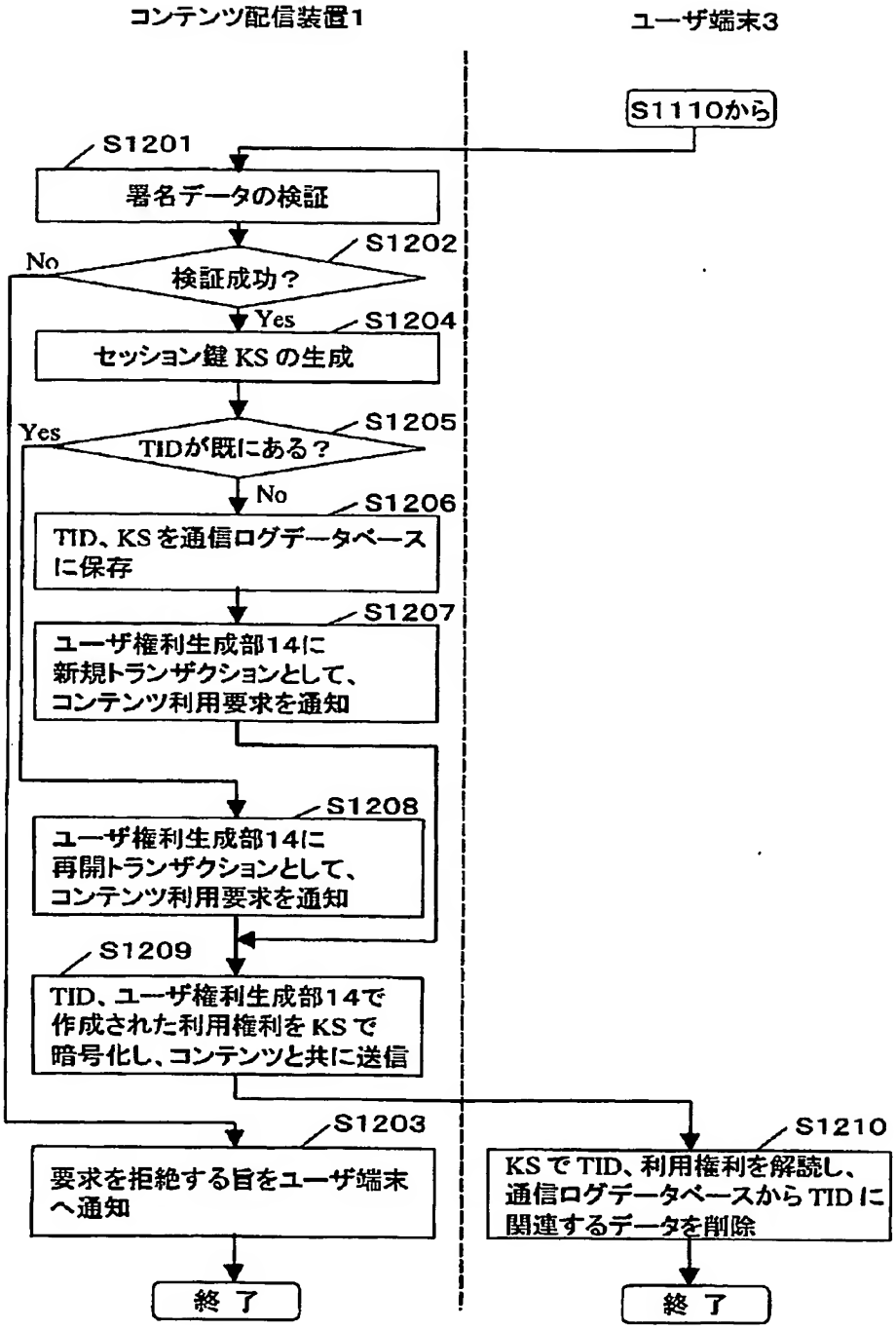
【図１０】


コンテンツ配信装置1
ユーザ端末3
開 始
S1001
乱数 Rc、端末公開鍵証明書、
コンテンツ利用要求を送信
S1002
端末公開鍵証明書の署名検証
No
S1003
検証成功？
Ycs
S1005
乱数 Rs、TID、パラメータ DHs の
生成
S1006
署名データ S(s, Rc‖TID‖DHs) の
生成
S1007
乱数 Rs、TID、パラメータ DHs、
署名データの送信
S1101へ
S1004
要求を拒絶する旨をユーザ端末
へ通知
終 了

【図１１】


コンテンツ配信装置1
ユーザ端末3
S1007から
S1101
サーバ公開鍵証明書の署名検証
S1102
検証成功？
No
Yes
S1104
署名データの検証
S1105
検証成功？
No
Yes
S1106
パラメータ DHc の生成
S1107
セッション鍵 KS の生成
S1108
TID、Rs、DHc、KS を通信ログデータベースに保存
S1109
署名データ S(c, Rs||TID||DHc) の生成
S1110
TID、パラメータ DHc、署名データの送信
S1201へ
S1103
要求を拒絶する旨をユーザ指示処理部31へ通知
終了

【図１２】


コンテンツ配信装置1
ユーザ端末3
S1110から
S1201
署名データの検証
S1202
No
検証成功？
Yes
S1204
セッション鍵 KS の生成
S1205
Yes
TIDが既にある？
No
S1206
TID、KS を通信ログデータベースに保存
S1207
ユーザ権利生成部14に新規トランザクションとして、コンテンツ利用要求を通知
S1208
ユーザ権利生成部14に再開トランザクションとして、コンテンツ利用要求を通知
S1209
TID、ユーザ権利生成部14で作成された利用権利を KS で暗号化し、コンテンツと共に送信
S1203
要求を拒絶する旨をユーザ端末へ通知
S1210
KS で TID、利用権利を解読し、通信ログデータベースから TID に関連するデータを削除
終了
終了

【書類名】　要約書

【要約】

【課題】　ＳＡＣプロトコルや通信切断対策プロトコルの双方を利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となるという課題があった。

【解決手段】　サーバ装置および端末装置間の通信に、少なくとも前記サーバ装置による前記端末装置の正当性の認証と通信暗号鍵の共有を行う認証フェーズを含み、前記認証フェーズには、前記サーバ装置と前記端末装置間で通信されるトランザクションを識別する情報を交換するトランザクション識別情報交換フェーズと、前記トランザクションにおける前記端末装置からの先頭のコマンドを送信する先頭コマンド送信フェーズとを含むことにより、ユーザに対する応答時間を削減する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０１７６３７
受付番号	５０３００１２４４５７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　１月２８日

＜認定情報・付加情報＞

【提出日】　平成15年 1月27日

次頁無

特願２００３－０１７６３７

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社